CLAIMS

1. Method of generating a cryptographic protocol between a first electronic entity (A) and a second electronic entity (B) subject to attack, according to which any message (M) is generated, on the basis of which a chain of operations is carried by the said second entity resulting in the generation of a resultant or response message (R), the said response being compared with the result of another similar processing applied to the said message and carried out by the said first entity, characterised in that, at least in certain stages of the said chain of operations, the said second entity carries out either an operation of a chosen type (O_1, O_2, O_3 … O_n) or the same operation complemented ($\overline{O}_1$, $\overline{O}_2$, $\overline{O}_3$ … $\overline{O}_n$), the choice depending on a random decision and in that the said response is constituted by the result of the last operation of the said chain, possibly complemented.

2. Method according to claim 1, characterised in that an operation capable of being complemented is the operation known as the exclusive OR.

3. Method according to claim 1 or 2, characterised in that an operation capable of being complemented is a known operation of permutation of the bits of the said message or of an intermediate result obtained on carrying out the said chain of operations.

4. Method according to one of claims 1 to 3, characterised in that an operation capable of being complemented is the operation known as indexed access to a table.

5. Method according to one of claims 1 to 4, characterised in that an operation capable of being complemented is a stable operation with respect to the application of the exclusive OR function.

6. Method according to claim 5, characterised in that an operation capable of being complemented is the transfer of the said message or of an intermediate result obtained whilst carrying out an operation of the said chain, from one location to another of a storage space.

7. Method according to one of the preceding claims, characterised in that consists in using the said message or an intermediate result resulting from the execution of a preceding operation of the said chain, in applying a new operation of the said chain to it, or this same operation complemented, depending on the state of a random parameter (S'_a) associated with this new operation, in updating a complementing counter (C_c) and in taking into account the state of this counter at the end of the execution of the said chain of operations in order to decide on the final configuration of the said response.

8. Method according to one of claims 1 to 6, characterised in that consists in using the said message, or an intermediate result of the execution of a preceding operation of the said chain, in applying to it a new operation of the said chain or this same operation complemented, depending on the state of a random parameter (S'_a) associated with this new operation and in transmitting, from operation to operation, information forming part of the said intermediate results, necessary for the final configuration of the said response.

9. Method according to one of claims 1 to 6, characterised in that there is defined in the said second entity two chains of operations (Ch_1, Ch_2) for the processing of the said message, one of the chains consisting of a series of data operations and the other chain consisting of a series of the same operations complemented and a final complementing (C) and in that it is decided randomly to execute one of the two chains of operations on each reception of a said message

10. Method according to one of the preceding claims, characterised in that, whilst the said series of operations is being carried out, there is computed the difference (d) between the number of times when the operations have been carried out in a normal fashion and the number of times when they have been carried out with complementing and in that the hazard (S'_a) is eliminated on the decision to carry out operations in a normal or complemented manner, in order to execute a certain number of subsequent operations, when the said difference exceeds a predetermined value, in the mode (normal or complemented) least used up to that point in view of reducing the said difference sufficiently.

11. Method according to one of the preceding claims, characterised in that the complementing is carried out byte by byte.

12. Method according to one of claims 1 to 10, characterised in that the complementing is carried out bit by bit.

13. Method according to one of the preceding claims, characterised in that, when several consecutive operations of the said chain are commutative, the order of their execution is permuted in a random manner.